REMARKS

A review of the claims indicates that:

A) Claims 2, 6, 9, 11-14, 36, 38, 58 and 63-69 remain in their original form.

B) Claims 17—31, 40—55 and 72—85 were previously withdrawn.

C) Claims 1, 3-5, 7, 32, 37, 56 and 57 are currently amended.

D) Claims 10, 16, 33-35, 39 and 59-62 are cancelled.

E) Claims 8, 15, 70 and 71 are previously presented.

In view of the following remarks, Applicant respectfully requests allowance of the non-withdrawn claims.

Section 101

Claim 32 was objected to as being directed to non-statutory subject matter. Without conceding the propriety of the rejection and only to advance the prosecution of this application, Applicant has amended Claim 32 to further clarify features of the claimed subject matter. The Applicant believes that the amendment overcomes the rejection.

Traversal of the §103 Rejections

Claims 1—6, 9, 10, 32—36, 38, 39 and 56—65 stand rejected under 35 U.S.C. §103(a) as being unpatentable over US 2003/0105980, hereinafter "Challener" in view of U.S. Pat. No. 7,205883, hereinafter "Bailey", further in view of U.S. Pat. No. 6,272,631, hereinafter "Thomlinson". In response, the Applicant respectfully traverses the rejection.

Additionally, Claim 16 (now incorporated by amendment into Claim 1) was rejected by the additional reference U.S. Patent Application 2003/0095685, hereinafter "Tewfik". The Applicant has amended Claim 1 to recite the elements of, and assume the scope of, Claim 16. Accordingly, the Applicant will address the Tewfik reference in the rejection of Claim 1, below.

Claim 1 recites a method comprising:

- creating a data structure including a plurality of user id-user key pairs, each user id-user key pair comprising a user id associated with one of a plurality of users and a user key comprising a master key and a keyed-hash message authentication code encrypted using a password associated with the one of the plurality of users;
- storing data watermarked using the master key;
- **receiving a user id and user password from one of the plurality of users;**
- **selecting a user key from the data structure based on the received user id;**
- **hashing the received password to produce a hash value;**
- **decrypting the selected user key using the hash value to reproduce the master key;**
- using the master key to access the watermarked data; and
- delivering the data structure to one or more of the plurality of users.

Claim 1 has been amended to recite the elements of Claim 16, now cancelled, and therefore assumes the scope of original Claim 16.

Claim 1 has been amended to recite a method wherein a plurality of user keys are each encrypted versions of the master key, and that decryption of any of the user keys (using a hash of that user's password as the decryption key) results in the master key. Thus, a data structure includes a plurality of copies of the master key, each encrypted according to each user's password's hash. The Applicant respectfully submits that such a method, involving selecting user keys from a data structure configured to include a different encryption of the master key for each user, is not taught or suggested by the prior art of record.

Challener, at Fig. 1, teaches the use of a table (e.g. a data structure) associating user IDs and a hash of a password. This is useful, in that a user will input the user's password, which is hashed, and then compared to the hash in the table. This is better than keeping the user's password in the table, since if the table is copies maliciously, the hashes in the table will not reveal the underlying passwords. However, Challener fails to teach or suggest a table which associates each user with a differently encrypted version of the master password, available to each of a plurality of users, and particularly wherein such a version was encrypted with the hash of the user's password.

Referring to Bailey, column 8 lines 7-25 teach that a SAK (secondary authentication key) can be wrapped/unwrapped (encrypted/decrypted) using the hash of a password as a key. However, Bailey fails to teach or suggest a plurality of differently encrypted versions of the master password, available to each of a plurality of users, and particularly wherein such a version was encrypted with the hash of the user's password.

Referring to Thomlinson at the Abstract and column 109 lines 1-63, Thomlinson teaches that all of a user's documents can be encrypted with a master key that do not have to be re-encrypted when the user changes his or her password (see column 10 lines 58-63). Thus, Thomlinson teaches that the "master password" is used to encrypt each of the user's documents, although the master key is actually used to decrypt the item key and authentication key, which are then used to decrypt the data item (column 10 lines 46-57). However, Thomlinson fails to teach or suggest a plurality of differently encrypted versions of the master password, available to each of a plurality of users, and particularly wherein such a version was encrypted with the hash of the user's password

Referring to Tewfik, watermarking of data is disclosed.

In making out the rejection of Claim 16, now cancelled and its elements recited by Claim 1, the Patent Office suggests that columns 9 and 10 of Thomlinson teaches storing data using the master key. However, the Applicant respectfully submits that the claim affirmatively states that the master password is effective for all users, while the prior art of record (i.e. Thomlinson, which teaches in this area) teaches that a master password is sufficient to decrypt all documents associated with a single user.

Referring again to Thomlinson at column 9 lines 59-65, Thomlinson discusses the item key (used to encrypt the data) and the authentication key (which is used to verify that the data is authentic once decrypted). Each data file is encrypted/decrypted with its own item key (Thomlinson, column 10, lines 10-14 and 56-57). This is in contrast to the recited language of the claim, wherein the selected user key is decrypted using the hash value to reproduce the master key. That is, in Thomlinson, the master key (which can decrypt any of the single user's many item keys, one associated with each data item) decrypts the item key, which decrypts the data. In the claim, the user key is decrypted by the hash of the password to result in the master key, which can decrypt any of many files (thus, it's called the master key).

The Applicant submits that the language of the claim make clear that any user, having the correct user ID and password, can access the master password, and can thereby decrypt any data. In contrast, Thomlinson teaches that a given user can access a master password, and can thereby decrypt any of the user's own files. This is because the claim recites that a plurality of user keys are each encrypted versions of the master key, and that decryption of any of the user keys (using a hash of that user's password as the decryption key) results in the master key.

Moreover, the Applicant submits that none of the art teaches of suggests that a single password (e.g. the "master password") is encrypted in a plurality of different ways, and is thereby made available to a plurality of different users. Claim 1, as amended, necessarily results in this situation, since "receiving a user id and user password from one of the plurality of users" allows "decrypting the selected user key using the hash value to reproduce the master key".

Therefore, the Applicant respectfully submits that Claim 1 recites elements not taught or suggested by Challener, Bailey and Thomlinson, and requests that the Section 103 rejection be removed.

Claims 2—9 and 11—15 depend from Claim 1 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features that, in combination with those recited in Claim 1, are neither taught nor suggested in references of record, either singly or in combination with one another. Accordingly, the Applicant respectfully requests that the Section 103 rejection of these claims be removed.

Claim 32 recites a computer readable medium having stored thereon computer executable instructions for performing acts comprising:

- accessing a user key associated with a user ID, wherein the accessing is from a user key data structure and is upon presentation of a user ID of a user, and wherein the user key data structure comprises a plurality of encryptions of a master key, and **wherein each of the plurality of encryptions of the master key is associated with one of a plurality of users, respectively**, and wherein each of the plurality of encryptions of the user master key was encrypted by operation of a reversible process using a hash value of a password of an associated user as a key in the reversible process;
- hashing, upon presentation of a password of the user, the presented password, to thereby produce a hash value;
- decrypting the user key using the hash value, thereby creating the master key; and
- decrypting data using the master key.

Claim 32 has been amended to recite "wherein each of the plurality of encryptions of the master key is associated with one of a plurality of users, respectively".

In contrast, Thomlinson discloses a master key that is adapted to allow a single user to open any of a plurality of files encrypted by that user. Bailey, at column 8, teaches that the SAK key can be encrypted and/or decrypted with a hashed password. Challener teaches that a table of user IDs and hashed passwords can protect data, since the hashed passwords cannot be reversed to obtain the passwords. However, none of the art teaches or suggests a "plurality of encryptions of the master key is associated with one of a plurality of users, respectively".

Because Claim 32 has been extensively amended, the Patent Office has not actually suggested that the prior art, noted above, actually teaches or suggests the elements recited by the amendments.

However, the Applicant respectfully submits that the prior art of record fails to teach or suggest a key (e.g. a master key) associated with a plurality of different encrypted versions of that key (e.g. user keys). In contrast, Challener teaches (Fig. 1) associating user IDs with hashed passwords, Bailey teaches (column 8 and 9, such as column 8 lines 7-25) the use of a hashed password to encrypt and/or decrypt a key, and Thomlinson teaches (column 10 lines 46-57) the use of a password to derive a user key, to thereby decrypt a master key suitable to decrypt any item key associated with a data item (file) associated with the user.

The Applicant, by amending Claim 32 to recite that "each of the plurality of encryptions of the master key is associated with one of a plurality of users, respectively", distinguishes the prior art of record. The prior art fails to teach or suggest such multiple different encryptions of a key, generally, and more specifically, associating each of the encryptions of the master key with one of a plurality of users.

Accordingly, the Applicant respectfully requests that the Patent Office remove the Section 103 rejection of Claim 32.

Claims 36-38 depend from Claim 32 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features that, in combination with those recited in Claim 32, are neither taught nor suggested in references of record, either singly or in combination with one another. Accordingly, the Applicant respectfully requests that the Section 103 rejection of these claims be removed.

Claim 56 recites a system comprising:

- means for **producing a plurality of user keys, wherein each user key is associated with one of a plurality of users, respectively, and wherein each of the plurality of user keys is an encryption of a single master key**, and wherein the encryption is by operation of a reversible process using a hash value of a different password associated with each user as a key in the reversible process;
- …

Claim 56 has been amended to recite "wherein each user key is associated with one of a plurality of users, respectively, and wherein each of the plurality of user keys is an encryption of a single master key". Accordingly, the Applicant respectfully submits that Claim 56 is allowable for at least the reasons that Claim 32 is allowable.

Claim 57 has been amended to recite "producing a plurality of user keys, wherein each user key is associated with one of a plurality of users, respectively, and wherein each of the plurality of user keys is an encryption of a single master key". Accordingly, the Applicant respectfully submits that Claim 56 is allowable for at least the reasons that Claim 32 is allowable.

Claims 58 and 63-71 depend from Claim 57 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features that, in combination with those recited in Claim 57, are neither taught nor suggested in references of record, either singly or in combination with one another. Accordingly, the Applicant respectfully requests that the Section 103 rejection of these claims be removed.

<u>Conclusion</u>

The Applicant submits that all of the claims are in condition for allowance and respectfully requests that a Notice of Allowability be issued. If the Office's next anticipated action is not the issuance of a Notice of Allowability, the Applicant respectfully requests that the undersigned attorney be contacted for the purpose of scheduling an interview.

Respectfully Submitted,

Dated: 29 September 2008

By: /David S. Thompson/
David S. Thompson
Reg. No. 37,954
Attorney for Applicant

LEE & HAYES PLLC
Suite 500
421 W. Riverside Avenue
Spokane, Washington 99201

Telephone: 509-324-9256 x235
Facsimile: (509) 323-8979